Complexité avancée - UMIN 345
Théorie de la NP-Complétude (2)

Christophe PAUL

September 24, 2007

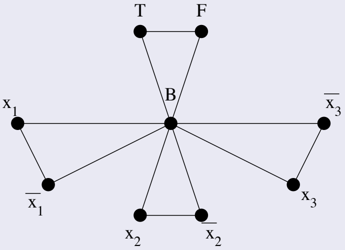
EXERCICE : Montrer que 3-SAT $\leqslant_K$ 3-COLORATION

EXERCICE : Montrer que 3-SAT $\leqslant_K$ 3-COLORATION

1. 3-COLORATION appartient clairement à **NP**
2. Construction d'un graphe à partir d'une instance $\mathcal{I}$ de 3-SAT:
   - V contient 3 sommets B, T et F ainsi que 2 sommets x_i et $\overline{x_i}$ pour chaque variable x_i.
   - **Observation:** $\forall i$, x_i et $\overline{x_i}$ sont coloriés différement par T et F.

EXERCICE : Montrer que 3-SAT $\leqslant_K$ 3-COLORATION

1. 3-COLORATION appartient clairement à **NP**
2. Construction d'un graphe à partir d'une instance $\mathcal{I}$ de 3-SAT:
   - V contient 3 sommets B, T et F ainsi que 2 sommets x_i et $\overline{x_i}$ pour chaque variable x_i.
   - $\{B, T, F\}$ est un triangle de G ainsi que $\forall i, \{B, x_i, \overline{x_i}\}$



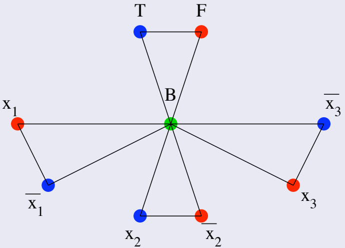
   - à chaque clause, on associe le gadget suivant

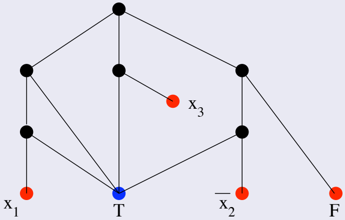
EXERCICE : Montrer que 3-SAT $\leqslant_K$ 3-COLORATION

1. 3-COLORATION appartient clairement à **NP**
2. Construction d'un graphe à partir d'une instance $\mathcal{I}$ de 3-SAT:
   - V contient 3 sommets B, T et F ainsi que 2 sommets x_i et $\overline{x_i}$ pour chaque variable x_i.
   - $\{B, T, F\}$ est un triangle de G ainsi que $\forall i, \{B, x_i, \overline{x_i}\}$

EXERCICE : Montrer que 3-SAT $\leqslant_K$ 3-COLORATION

1. 3-COLORATION appartient clairement à **NP**
2. Construction d'un graphe à partir d'une instance $\mathcal{I}$ de 3-SAT

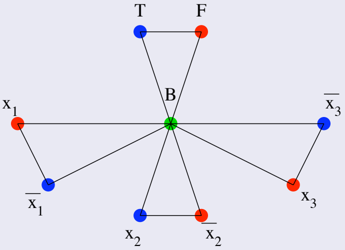


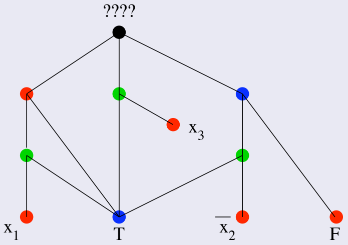


3. G est 3-coloriable ssi $\mathcal{I}$ est satisfiable
   - Si aucun terme de la clause reçoit la couleur T, alors le graphe n'est pas 3-coloriable.

EXERCICE : Montrer que 3-SAT $\leqslant_K$ 3-COLORATION

1. 3-COLORATION appartient clairement à **NP**
2. Construction d'un graphe à partir d'une instance $\mathcal{I}$ de 3-SAT

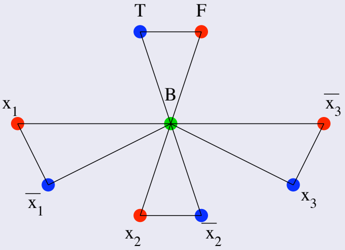


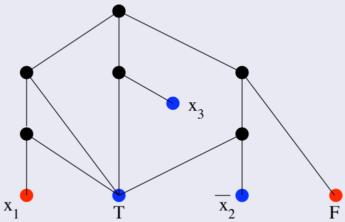


3. G est 3-coloriable ssi $\mathcal{I}$ est satisfiable
   - Si aucun terme de la clause reçoit la couleur T, alors le graphe n'est pas 3-coloriable.

Exercice : Montrer que 3-SAT $\leqslant_K$ 3-COLORATION

1. 3-COLORATION appartient clairement à **NP**
2. Construction d'un graphe à partir d'une instance $\mathcal{I}$ de 3-SAT

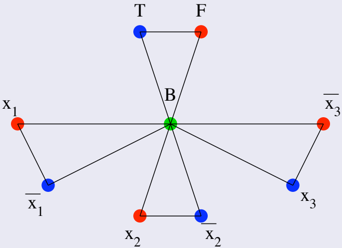


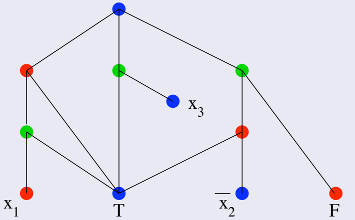


3. G est 3-coloriable ssi $\mathcal{I}$ est satisfiable
   - Si aucun terme de la clause reçoit la couleur T, alors le graphe n'est pas 3-coloriable.
   - Si au moins un terme de la clause reçoit la couleur T, alors le graphe est 3-coloriable.

EXERCICE : Montrer que 3-SAT $\leqslant_K$ 3-COLORATION

1. 3-COLORATION appartient clairement à **NP**
2. Construction d'un graphe à partir d'une instance $\mathcal{I}$ de 3-SAT

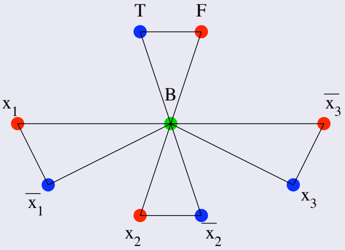


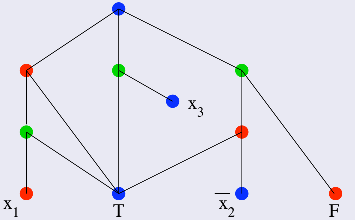


3. G est 3-coloriable ssi $\mathcal{I}$ est satisfiable
   - Si aucun terme de la clause reçoit la couleur T, alors le graphe n'est pas 3-coloriable.
   - Si au moins un terme de la clause reçoit la couleur T, alors le graphe est 3-coloriable.

EXERCICE : Montrer que 3-SAT $\leqslant_K$ 3-COLORATION

1. 3-COLORATION appartient clairement à **NP**
2. Construction d'un graphe à partir d'une instance $\mathcal{I}$ de 3-SAT





3. G est 3-coloriable ssi $\mathcal{I}$ est satisfiable
   - Si aucun terme de la clause reçoit la couleur T, alors le graphe n'est pas 3-coloriable.
   - Si au moins un terme de la clause reçoit la couleur T, alors le graphe est 3-coloriable.
4. La construction du graphe est clairement polynomiale.

Un autre exemple

1. CYCLE : Etant donnés un graphe G et deux sommets x et y, existe-t-il un cycle passant par x et y ?

Un autre exemple

1. CYCLE : Etant donnés un graphe G et deux sommets x et y, existe-t-il un cycle passant par x et y ?

CYCLE appartient à **P**

Un autre exemple

1. CYCLE : Etant donnés un graphe G et deux sommets x et y, existe-t-il un cycle passant par x et y ?

   CYCLE appartient à **P**

2. CIRCUIT : Etant donnés un graphe **orienté** $\overrightarrow{H}$ et deux sommets x et y, existe-t-il un **circuit** passant par x et y ?

Un autre exemple

1. CYCLE : Etant donnés un graphe G et deux sommets x et y, existe-t-il un cycle passant par x et y ?

   CYCLE appartient à **P**

2. CIRCUIT : Etant donnés un graphe **orienté** $\overrightarrow{H}$ et deux sommets x et y, existe-t-il un **circuit** passant par x et y ?

   CIRCUIT appartient à **NP**(cf problème du LINKAGE)

Travail à rendre (pour le 1er octobre 2007)

Montrer que le problème COUPLAGE TRI-PARTI est **NP**-complet.

- **Donnée :** Un ensemble T de triplets de $B \times G \times H$ avec B, G, H des ensembles à n éléments.
- **Question :** Existe-t-il un sous-ensemble $S \subseteq T$ de n triplets deux à deux disjoints ?

- Pourra rapporter jusque 3 points de bonus pour l'examen.
- Travail en groupe possible, **mais** :
  1. indiquez avec qui vous avez travaillé;
  2. chacun rend sa propre copie;
- Si vous utiliser des sources bibliographiques, il faut les référencer.

La classe coNP

La classe co-**NP** contient les problèmes pour lesquels il existe un certificat polynomial pour les instances **négatives**

La classe co**NP**

La classe co-**NP** contient les problèmes pour lesquels il existe un certificat polynomial pour les instances **négatives**

Exemple: PREMIER

- **Problème:** Décider si un entier n est premier
- **Certificat négatif:** une factorisation de n

Lemma

Si un problème Π appartient à **NP**, alors le problème complémentaire $\overline{\Pi}$ appartient à co**NP**.

Lemma

Si un problème Π appartient à **NP**, alors le problème complémentaire $\overline{\Pi}$ appartient à co**NP**.

Exemple: CHEMIN HAMILTONIEN

- **Problème:** Décider si un graphe G ne contient pas de chemin hamiltonien.
- **Certificat négatif:** un chemin hamiltonien!

co**NP**-complet

Un problème Π est co**NP**-complet si tout problème Π' de co**NP** satisfait $\Pi' \leqslant_K \Pi$.

co**NP**-complet

Un problème Π est co**NP**-complet si tout problème Π' de co**NP** satisfait $\Pi' \leqslant_K \Pi$.

Théorème

Si un problème co**NP**-complet Π appartient à **NP**, alors **NP**=co-**NP**.

co**NP**-complet

Un problème Π est co**NP**-complet si tout problème Π' de co**NP** satisfait $\Pi' \leqslant_K \Pi$.

Théorème

Si un problème co**NP**-complet Π appartient à **NP**, alors **NP**=co-**NP**.

1. Montrons que si $\Pi \in$ **NP** est co**NP**-complet, alors co**NP** $\subseteq$ **NP**.

co**NP**-complet

Un problème Π est co**NP**-complet si tout problème Π' de co**NP** satisfait $\Pi' \leqslant_K \Pi$.

Théorème

Si un problème co**NP**-complet Π appartient à **NP**, alors **NP**=co-**NP**.

1. Montrons que si $\Pi \in$ **NP** est co**NP**-complet, alors co**NP** $\subseteq$ **NP**.
   - Soit $\Pi' \in$ co**NP**. Π est co**NP**-complet $\Rightarrow \Pi' \leqslant_K \Pi$
   - Donc il existe une réduction de Π' vers Π.

coNP-complet

Un problème Π est co**NP**-complet si tout problème Π' de co**NP** satisfait $\Pi' \leqslant_K \Pi$.

Théorème

Si un problème co**NP**-complet Π appartient à **NP**, alors **NP**=co-**NP**.

1. Montrons que si $\Pi \in$ **NP** est co**NP**-complet, alors co**NP** $\subseteq$ **NP**.
   - Soit $\Pi' \in$ co**NP**. Π est co**NP**-complet $\Rightarrow \Pi' \leqslant_K \Pi$
   - Donc il existe une réduction de Π' vers Π.
   - Π' peut être résolu de manière non-déterministe polynomiale grâce à cette réduction et un algorithme non-déterministe polynomial pour Π.

co**NP**-complet

Un problème Π est co**NP**-complet si tout problème Π' de co**NP** satisfait $\Pi' \leqslant_K \Pi$.

Théorème

Si un problème co**NP**-complet Π appartient à **NP**, alors **NP**=co-**NP**.

1. Montrons que si $\Pi \in$ **NP** est co**NP**-complet, alors co**NP** $\subseteq$ **NP**.
    - Soit $\Pi' \in$ co**NP**. Π est co**NP**-complet $\Rightarrow \Pi' \leqslant_K \Pi$
    - Donc il existe une réduction de Π' vers Π.
    - Π' peut être résolu de manière non-déterministe polynomiale grâce à cette réduction et un algorithme non-déterministe polynomial pour Π.
2. L'égalité est prouvée par symétrie.

Problème ouvert

Est-ce que **NP** $=$ co-**NP** ?

Problème ouvert

Est-ce que **NP** $=$ co-**NP** ?

Théorème

Si **NP** $\neq$ co-**NP**, alors **P** $\neq$ **NP**.

Problème ouvert

Est-ce que **NP** $=$ co-**NP** ?

Théorème

Si **NP** $\neq$ co-**NP**, alors **P** $\neq$ **NP**.

- On montre que si **P** $=$ **NP**, alors **NP** $=$ co-**NP**.

Problème ouvert

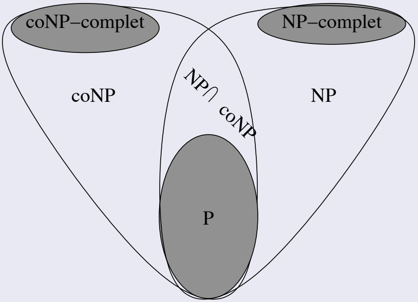
Est-ce que **NP** $=$ co-**NP** ?

Théorème

Si **NP** $\neq$ co-**NP**, alors **P** $\neq$ **NP**.

- On montre que si **P** $=$ **NP**, alors **NP** $=$ co-**NP**.
- L'idée est que **P** $=$ co-**P**...

Relation entre les classes de complexité



Il est clair que $\mathbf{P} \subseteq \mathbf{NP} \cap \mathrm{co}\mathbf{NP}$.

Problème ouvert

Est-ce que $\mathbf{P} = \mathbf{NP} \ \cap$ co-$\mathbf{NP}$?

Retour sur PREMIER

- On a vu que PREMIER appartient à co$\mathbf{NP}$.

Problème ouvert

Est-ce que **P** = **NP** ∩ co-**NP** ?

Retour sur PREMIER

- On a vu que PREMIER appartient à co**NP**.
- **Théorème de Pratt (1975) :**
  Tout nombre premier possède un certificat positif.

Problème ouvert

Est-ce que **P** $=$ **NP** $\cap$ co-**NP** ?

Retour sur PREMIER

- On a vu que PREMIER appartient à co**NP**.
- **Théorème de Pratt (1975) :**
  Tout nombre premier possède un certificat positif.
- PREMIER est longtemps resté dans la classe **NP** $\cap$ co-**NP**.

Problème ouvert

Est-ce que **P** $=$ **NP** $\cap$ co-**NP** ?

Retour sur PREMIER

- On a vu que PREMIER appartient à co**NP**.
- **Théorème de Pratt (1975) :**
  Tout nombre premier possède un certificat positif.
- PREMIER est longtemps resté dans la classe **NP** $\cap$ co-**NP**.
- Il appartient à **P** depuis quelques années [Agrawal, Saxena et Kayal, 2002].

Bonnes caractérisations - la classe **NP** $\cap$ co-**NP**

NP $\cap$ co-**NP** est la classe de problèmes pour lesquels il existe un certificat positif et un certificat négatif.

- Théorèmes min-max : flôt maximum - coupe minimum...

Bonnes caractérisations - la classe NP $\cap$ co-NP

NP $\cap$ co-**NP** est la classe de problèmes pour lesquels il existe un certificat positif et un certificat négatif.

- Théorèmes min-max : flôt maximum - coupe minimum...

Problèmes de NP $\cap$ coNP non connus pour être dans P

- PARITY GAME
- TRANSVERSAL MINIMUM
  - **Données:** $B = (X, Y, E)$ un graphe biparti et $F \subseteq 2^X$
  - **Question:** F est-il l'ensemble des transversaux minimaux (pour l'inclusion) de B

  Un ensembe $T \subseteq X$ est un transversal de B si $N(T) = Y$
- ...

Un exemple de bonne caractérisation: COUPLAGE PARFAIT

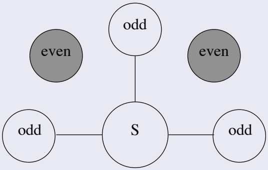
- **Données :** Un graphe $G = (V, E)$ à n sommets
- **Question :** Existe-t-il un couplage parfait ($\frac{n}{2}$ arêtes deux à deux disjointes)

Un exemple de bonne caractérisation: COUPLAGE PARFAIT

- **Données :** Un graphe $G = (V, E)$ à n sommets
- **Question :** Existe-t-il un couplage parfait ($\frac{n}{2}$ arêtes deux à deux disjointes)

Observation

Si il existe un ensembe $S \subseteq V$ tel que $|S| < odd(G - S)$, alors G ne possède pas de couplage parfait.

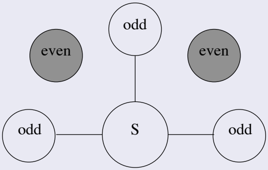


Un exemple de bonne caractérisation: COUPLAGE PARFAIT

- **Données :** Un graphe $G = (V, E)$ à n sommets
- **Question :** Existe-t-il un couplage parfait ($\frac{n}{2}$ arêtes deux à deux disjointes)

Observation

Si il existe un ensembe $S \subseteq V$ tel que $|S| < odd(G - S)$, alors G ne possède pas de couplage parfait.



$\Rightarrow$ COUPLAGE PARFAIT $\in$ **NP** $\cap$ co**NP**

Théorème [Tutte, 1947]

Un graphe $G = (V, E)$ possède un couplage parfait ssi

$$\forall S \subseteq V, odd(G-S) \leqslant |S| \qquad \mathbf{(1)}$$

Théorème [Tutte, 1947]

Un graphe $G = (V, E)$ possède un couplage parfait ssi

$$\forall S \subseteq V, odd(G - S) \leqslant |S| \qquad \textbf{(1)}$$

Preuve

Hypothèses : G vérifie (1), ne possède pas de couplage parfait mais $\forall xy \notin E$, $G + xy$ possède un couplage parfait.

Remarque: $|V|$ est pair

Théorème [Tutte, 1947]

Un graphe $G = (V, E)$ possède un couplage parfait ssi

$$\forall S \subseteq V, odd(G - S) \leqslant |S| \qquad \textbf{(1)}$$

Preuve

Hypothèses : G vérifie (1), ne possède pas de couplage parfait mais $\forall xy \notin E$, $G + xy$ possède un couplage parfait.

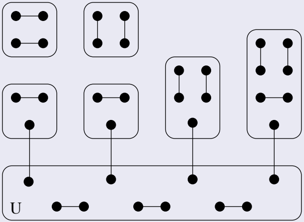
Remarque: $|V|$ est pair Soit U l'ensemble des sommets universels de G

Théorème [Tutte, 1947]

Un graphe $G = (V, E)$ possède un couplage parfait ssi
$$\forall S \subseteq V, odd(G - S) \leqslant |S| \qquad \textbf{(1)}$$

Preuve

1. Si $G - U$ est une union disjointe de cliques



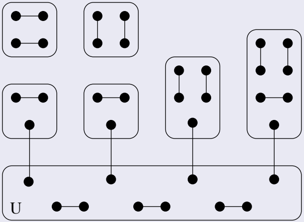
Théorème [Tutte, 1947]

Un graphe $G = (V, E)$ possède un couplage parfait ssi

$$\forall S \subseteq V, odd(G - S) \leqslant |S| \qquad \mathbf{(1)}$$

Preuve

1. Si $G - U$ est une union disjointe de cliques



$\Rightarrow$ il existe un couplage parfait

Théorème [Tutte, 1947]

Un graphe $G = (V, E)$ possède un couplage parfait ssi

$$\forall S \subseteq V, odd(G - S) \leqslant |S| \qquad \textbf{(1)}$$

Preuve

1. Si $G - U$ est une union disjointe de cliques
2. Sinon, $G - U$ contient un chemin sans corde x, y, z et un sommet z non voisin de y.
   - $G + xz$ $(G + yw)$ possède un couplage parfait M_{xz} (M_{yw}) Soit l'ensemble d'arêtes $F = (M_{xy} \Delta M_{yw})$

Théorème [Tutte, 1947]

Un graphe $G = (V, E)$ possède un couplage parfait ssi

$$\forall S \subseteq V, odd(G - S) \leqslant |S| \qquad \textbf{(1)}$$

Preuve

1. Si $G - U$ est une union disjointe de cliques
2. Sinon, $G - U$ contient un chemin sans corde x, y, z et un sommet z non voisin de y.
   - $G + xz$ $(G + yw)$ possède un couplage parfait M_{xz} (M_{yw}) Soit l'ensemble d'arêtes $F = (M_{xy} \Delta M_{yw})$
   - $F =$ union de cycles et de points isolés. Soit C le cycle de xz.

Théorème [Tutte, 1947]

Un graphe $G = (V, E)$ possède un couplage parfait ssi

$$\forall S \subseteq V, odd(G - S) \leqslant |S| \qquad \textbf{(1)}$$

Preuve

1. Si $G - U$ est une union disjointe de cliques
2. Sinon, $G - U$ contient un chemin sans corde x, y, z et un sommet z non voisin de y.
   - $G + xz$ ($G + yw$) possède un couplage parfait M_{xz} (M_{yw})
     Soit l'ensemble d'arêtes $F = (M_{xy} \Delta M_{yw})$
   - $F =$ union de cycles et de points isolés. Soit C le cycle de xz.
   - Si C ne contient pas $yw \Rightarrow \exists$ un couplage parfait dans G.
     Il suffit de mixer les couplages M_{xz} et M_{yz} selon les cycles.

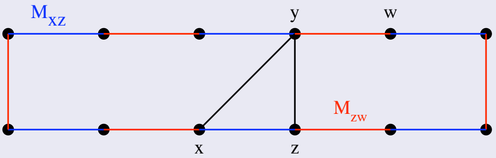
Théorème [Tutte, 1947]

Un graphe $G = (V, E)$ possède un couplage parfait ssi

$$\forall S \subseteq V, odd(G - S) \leqslant |S| \qquad \textbf{(1)}$$

Preuve

1. Si $G - U$ est une union disjointe de cliques
2. Sinon, $G - U$ contient un chemin sans corde x, y, z et un sommet z non voisin de y.
   - $G + xz$ $(G + yw)$ possède un couplage parfait M_{xz} (M_{yw}) Soit l'ensemble d'arêtes $F = (M_{xy} \Delta M_{yw})$
   - F = union de cycles et de points isolés. Soit C le cycle de xz.
   - Sinon on trouve un autre couplage parfait:



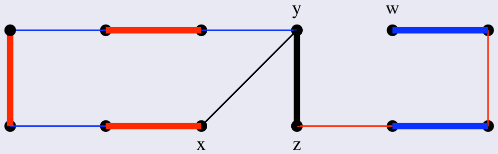
Théorème [Tutte, 1947]

Un graphe $G=(V,E)$ possède un couplage parfait ssi

$$\forall S \subseteq V, odd(G-S) \leqslant |S| \qquad \textbf{(1)}$$

Preuve

1. Si $G-U$ est une union disjointe de cliques
2. Sinon, $G-U$ contient un chemin sans corde x,y,z et un sommet z non voisin de y.
   - $G+xz$ $(G+yw)$ possède un couplage parfait M_{xz} (M_{yw}) Soit l'ensemble d'arêtes $F=(M_{xy}\Delta M_{yw})$
   - $F=$ union de cycles et de points isolés. Soit C le cycle de xz.
   - Sinon on trouve un autre couplage parfait:



Théorème [Tutte, 1947]

Un graphe $G = (V, E)$ possède un couplage parfait ssi

$$\forall S \subseteq V, odd(G-S) \leqslant |S| \qquad \textbf{(1)}$$

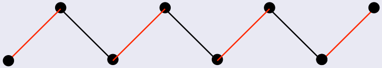
Corollaire [Berge, 1958]

Le nombre maximum de sommets dans un couplage de G est

$$min_{S\subseteq V}\{n-d(S)\}, \text{ avec } d(S) = odd(G-S) - |S|$$

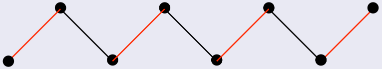
Lemme [Berge, 1957]

Un couplage M d'un graph G est maximum ssi G ne possède pas de chemin M-augmentant.



Lemme [Berge, 1957]

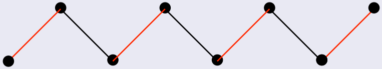
Un couplage M d'un graph G est maximum ssi
G ne possède pas de chemin M-augmentant.



$\Rightarrow$ Si on a un algorithme pour trouver un chemin augmentant, on montre que COUPLAGE PARFAIT est dans **P**.

Lemme [Berge, 1957]

Un couplage M d'un graph G est maximum ssi
G ne possède pas de chemin M-augmentant.



$\Rightarrow$ Si on a un algorithme pour trouver un chemin augmentant, on montre que COUPLAGE PARFAIT est dans **P**.

Edmond's blossom algorithm [1965]

- Edmonds $\longrightarrow O(n^4)$
  (implémentation en $O(n^3)$ [Ahuja, Magnanti, Orlin, 1993])
- Even-Kariv [1975] $\longrightarrow O(n^{5/2})$
- Micali, Vazirani [1980] $\longrightarrow O(n^{1/2}m)$

Un cas bizarre

1. ISOMORPHISME DE GRAPHE : Etant donnés deux graphes G_1 et G_2, existe-t-il un isomorphisme entre G_1 et G_2, i.e. une fonction

$$f : V_1 \longrightarrow V_2 \text{ telle que } xy \in E_1 \Leftrightarrow f(x)f(y) \in E_2$$

Un cas bizarre

1. ISOMORPHISME DE GRAPHE : Etant donnés deux graphes G_1 et G_2, existe-t-il un isomorphisme entre G_1 et G_2, i.e. une fonction

$$f : V_1 \longrightarrow V_2 \text{ telle que } xy \in E_1 \Leftrightarrow f(x)f(y) \in E_2$$

2. ISOMORPHISME $\in$ **NP**

Un cas bizarre

1. ISOMORPHISME DE GRAPHE : Etant donnés deux graphes G_1 et G_2, existe-t-il un isomorphisme entre G_1 et G_2, i.e. une fonction

$$f : V_1 \rightarrow V_2 \text{ telle que } xy \in E_1 \Leftrightarrow f(x)f(y) \in E_2$$

2. ISOMORPHISME $\in$ **NP**
3. ISOMORPHISME $\in$ **P** ?

Un cas bizarre

1. ISOMORPHISME DE GRAPHE : Etant donnés deux graphes G_1 et G_2, existe-t-il un isomorphisme entre G_1 et G_2, i.e. une fonction

$$f : V_1 \rightarrow V_2 \text{ telle que } xy \in E_1 \Leftrightarrow f(x)f(y) \in E_2$$

2. ISOMORPHISME $\in$ **NP**
3. ISOMORPHISME $\in$ **P** ?
4. ISOMORPHISME $\in$ **NP**-complet ?

Un cas bizarre

1. ISOMORPHISME DE GRAPHE : Etant donnés deux graphes G_1 et G_2, existe-t-il un isomorphisme entre G_1 et G_2, i.e. une fonction

$$f : V_1 \rightarrow V_2 \text{ telle que } xy \in E_1 \Leftrightarrow f(x)f(y) \in E_2$$

2. ISOMORPHISME $\in$ **NP**
3. ISOMORPHISME $\in$ **P** ?
4. ISOMORPHISME $\in$ **NP**-complet ?

Théorème

Si **P** $\neq$ **NP**, alors il existe un problème Π qui n'est ni dans **P** ni dans **NP**-complet.

La classe PEspace

Un problème Π est dans **PEspace** s'il existe un algorithme déterministique le résolvant qui utilise un espace de taille polynomial en la taille de la donnée

La classe PEspace

Un problème Π est dans **PEspace** s'il existe un algorithme déterministique le résolvant qui utilise un espace de taille polynomial en la taille de la donnée

Lemme

La classe **PEspace** contient la classe **P**.

La classe **PEspace**

Un problème Π est dans **PEspace** s'il existe un algorithme déterministique le résolvant qui utilise un espace de taille polynomial en la taille de la donnée

Lemme

La classe **PEspace** contient la classe **P**.

Un exemple d'algorithme de **PEspace**

Ecrire tous les entiers de 0 à $2^n - 1$ en binaire.

Exercice

Montrer que SAT $\in$ **PEspace**.

Exercice

Montrer que $\textsc{SAT} \in$ **PEspace**.

- Brute-force : on essaie toutes les solutions les unes après les autres.

Exercice

Montrer que SAT $\in$ **PEspace**.

- Brute-force : on essaie toutes les solutions les unes après les autres.
- Pour chaque instanciation des variables, on a besoin d'un espace $O(n)$ bits.

Exercice

Montrer que $\textsc{SAT} \in$ **PEspace**.

- Brute-force : on essaie toutes les solutions les unes après les autres.
- Pour chaque instanciation des variables, on a besoin d'un espace $O(n)$ bits.

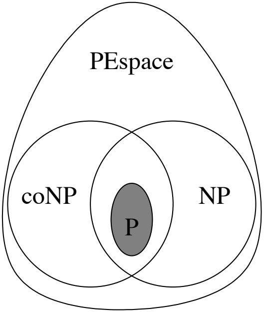
Conséquence

$\textsc{SAT} \in$ **NP**-complete et $\textsc{SAT} \in$ **PEspace** implique:

$$\mathbf{NP} \subseteq \mathbf{PEspace}$$

La classe **PEspace**-complet

Un problème Π appartient à **PEspace**-complet si Π appartient à **PEspace** et pour tout problème $\Pi' \in$ **PEspace**, $\Pi \leqslant_K \Pi'$.



SAT quantifié (QSAT)

- **Donnée :** $\Phi(x_1, \dots x_{2n+1})$ une formule booléenne (disjonction de clauses à 3 littéraux, 3-SAT)
- **Question :** $\exists x_1, \forall x_2 \dots \forall x_{2n}, \exists x_{2n+1} \Phi(x_1, \dots x_{2n+1})$?

SAT quantifié (QSAT)

- **Donnée :** $\Phi(x_1, \dots x_{2n+1})$ une formule booléenne (disjonction de clauses à 3 littéraux, 3-SAT)
- **Question :** $\exists x_1, \forall x_2 \dots \forall x_{2n}, \exists x_{2n+1} \Phi(x_1, \dots x_{2n+1})$?

Complexité de QSAT ? Est-ce que QSAT $\in$ **PEspace**?

SAT quantifié (QSAT)

- **Donnée :** $\Phi(x_1, \ldots x_{2n+1})$ une formule booléenne (disjonction de clauses à 3 littéraux, 3-SAT)
- **Question :** $\exists x_1, \forall x_2 \ldots \forall x_{2n}, \exists x_{2n+1} \Phi(x_1, \ldots x_{2n+1})$?

Complexité de QSAT ? Est-ce que QSAT $\in$ **PEspace**?

- Solution brute-force: $s(n) \leqslant 2s(n-1) + p(n) \Rightarrow$ espace exponentiel

SAT quantifié (QSAT)

- **Donnée :** $\Phi(x_1, \dots x_{2n+1})$ une formule booléenne (disjonction de clauses à 3 littéraux, 3-SAT)
- **Question :** $\exists x_1, \forall x_2 \dots \forall x_{2n}, \exists x_{2n+1} \Phi(x_1, \dots x_{2n+1})$?

Complexité de QSAT ? Est-ce que QSAT $\in$ **PEspace**?

- Solution brute-force: $s(n) \leqslant 2s(n-1) + p(n) \Rightarrow$ espace exponentiel
- Réutilisation de l'espace: $s(n) \leqslant s(n-1) + p(n) \leqslant np(n) \Rightarrow$ $\in$ **PEspace**

SAT quantifié (QSAT)

- **Donnée :** $\Phi(x_1, \ldots x_{2n+1})$ une formule booléenne (disjonction de clauses à 3 littéraux, 3-SAT)
- **Question :** $\exists x_1, \forall x_2 \ldots \forall x_{2n}, \exists x_{2n+1} \Phi(x_1, \ldots x_{2n+1})$?

Complexité de QSAT ? Est-ce que QSAT $\in$ **PEspace**?

- Solution brute-force: $s(n) \leqslant 2s(n-1) + p(n) \Rightarrow$ espace exponentiel
- Réutilisation de l'espace: $s(n) \leqslant s(n-1) + p(n) \leqslant np(n) \Rightarrow$ $\in$ **PEspace**

QSAT est **PEspace**-complet.

Décider, trouver...enumérer (ou compter)

- **Problème d'énumération :** Etant donné un problème Π et une instance $\mathcal{I}$, quel est le nombre de solutions $|\mathcal{S}(\mathcal{I})|$?

Décider, trouver. . . enumérer (ou compter)

- **Problème d'énumération :** Etant donné un problème Π et une instance $\mathcal{I}$, quel est le nombre de solutions $|\mathcal{S}(\mathcal{I})|$?
- Un problème Π appartient à la classe $\#$**P** s'il existe un algorithme non-déterministe $\mathcal{A}$ de décision tel que pour une instance $\mathcal{I}$, il y ait $|\mathcal{S}(\mathcal{I})|$ "possibilités" d'acceptation en temps polynomial en la taille de $\mathcal{I}$.

Décider, trouver. . . enumérer (ou compter)

- **Problème d'énumération :** Etant donné un problème Π et une instance $\mathcal{I}$, quel est le nombre de solutions $|\mathcal{S}(\mathcal{I})|$?
- Un problème Π appartient à la classe $\#\mathbf{P}$ s'il existe un algorithme non-déterministe $\mathcal{A}$ de décision tel que pour une instance $\mathcal{I}$, il y ait $|\mathcal{S}(\mathcal{I})|$ "possibilités" d'acceptation en temps polynomial en la taille de $\mathcal{I}$.
- une transformation polynomiale de Π vers Π' est **parcimonieuse** ssi pour une instance $\mathcal{I}$ de Π, alors $|\mathcal{S}(\mathcal{I})| = |\mathcal{S}(\mathcal{I}')|$.

Théorème [Simon, 1975]

Le problème de compter le nombre de solution de SAT est $\#\mathbf{P}$-complet.

Théorème [Simon, 1975]

Le problème de compter le nombre de solution de SAT est $\#\mathbf{P}$-complet.

1. Est-ce que problème $\Pi \in \mathbf{P}$ peut être $\#\mathbf{P}$-complet ?

Théorème [Simon, 1975]

Le problème de compter le nombre de solution de SAT est #**P**-complet.

1. Est-ce que problème $\Pi \in$**P** peut être #**P**-complet ? **OUI :** compter le nombre de couplages parfaits d'un graphe biparti.

Théorème [Simon, 1975]

Le problème de compter le nombre de solution de SAT est #**P**-complet.

1. Est-ce que problème $\Pi \in$**P** peut être #**P**-complet ? **OUI :** compter le nombre de couplages parfaits d'un graphe biparti.
2. En fait nombres de réductions polynomiales classiques sont parcimonieuses
   Exercice : vérifier si les réductions cues en cours sont parcimonieuses.